

Hackers

Continued from Page 8

"Chronos isn't old enough to drink?" asked the reporter.

"Chronos isn't old enough to drive," said Cruiser.

In the nascent age of computers the word "hacker" described a technological prodigy who, through the sheer force of his intelligence and imagination, was walking point for a young and expanding computer revolution. Minds honed on video games soon were designing intricate computer programs.

With the home-computer age, any kid with an inclination and parents well-off enough to buy him a disk drive and a modem, was free to explore and expand the outer edge of his computer potential. Those with a technological bent quickly got bored logging on to bulletin board systems where they could exchange messages and trade information with other computer users. They wanted to go where no hacker had gone before.

In 1983, the movie "War Games" starred Matthew Broderick as a high school hacker who nearly causes World War III. This was nothing short of epiphany for many young computer users. The movie spawned a legion of "rodents" — as their older, more learned hackers would come to call them. Learning ways of getting into other computer systems was fun, exciting, a source of intrigue and something to brag about to your friends.

In the early 1980s, the few laws involving hacking were vague at best. Those in the know could explore electronic space or "cyberspace" (a word coined by science-fiction author William Gibson in his book "Neuromancer") like cowboy rocketeers in new galaxies. Hackers found each other on computer bulletin boards and began sharing information. Groups like the infamous 2300 Club in Cleveland, the 414's from Milwaukee, and the Legion of Doom from all over the country, formed to collect as much information as possible about "secure" systems. This meant hacking their way through networks and into all kinds of government and corporate institutions.

The members of these disbanded groups are now legend in computer-hacking lore. Many have gone on to work for large corporations in their computer security divisions. Four members of the Legion of Doom, who were arrested in 1990 in the Secret Service's Operation Sundevil for entering a computer owned by BellSouth, have formed their own company, Comsec Data Security, to help private businesses secure their systems.

We don't live by 'Just say no.' We live by 'Just say know.'

Sitting at a coffee-shop counter, the reporter recognized Cruiser and Chronos immediately. They were fresh-faced, white, suburban boys who nearly shined with a combination of intelligence and naivete.

After a booth in the back was secured and an order for coffee was taken, Cruiser made an announcement. "This is the first time we've ever met in real space," he said, pointing to Chronos. He explained the difference between real space and cyberspace, the electronic environment of the computer on which they had communicated for almost a year.

Hackers, they said, were getting a bad name. There were precise distinctions to be made between hackers,

Hacker: Originally, a hard-core computer programmer. Has come to mean a person who creatively explores computer programs. More recently it has had a negative connotation meaning computer vandal, someone who damages systems or steals classified information.

Phone Phreaking: Using the phone system for free calls or other services.

Cracker: A hacker who intentionally destroys systems or uses his computer knowledge for ill-gotten gain or revenge. A bad hacker.

Virus: A program that replicates itself after it has been introduced into a computer, resulting in system problems or destruction.

Worm: A program that self-replicates rapidly enough to slow or stop whole computer systems.

The Lexicon Of Hacking

Bomb: A program that, when activated, destroys the computer system.

Social Engineering: Employing various ruses over the phone to get information that will allow an unauthorized person on a computer system.

How A Hacker Hacks: A hacker uses a modem to call the mainframe of a computer system. The system asks for a password. The hacker tries various common passwords such as "guest," "test" or "sysop" (system operator) until granted entrance. Once in the system, the hacker looks for an account that hasn't been used in awhile. The hacker finds that account's password and assumes that account's identity. It can take anywhere from a minute to a month to break into a system.

— M.H.

like themselves, who were merely exploring systems to increase their knowledge of computers, and "crackers," who were malicious vandals out to destroy for their own entertainment.

"People who are down on hackers are really out of touch," said Cruiser. "Hacking is really a good thing. Hacking inspires creativity. Hackers are guys who are bored with school, typical underachievers. Besides letting people know their systems aren't secure, it's an intellectual exercise. ...

"I see hackers as the next generation of counterculture. Like techno-hippies. There are all kinds of hackers — from art punks to metalheads to geeks. But what matters is we all live and communicate in the same computer network. We don't live by 'Just say no.' We live by 'Just say know.' Knowledge is where it's at for hackers."

But if hacking is such a divinely benevolent activity, why do so many people regard the practitioners with fear and menace?

"People are afraid of computers," Cruiser said. "They don't even want to know how much of their lives are already dominated by computers, how much of their personal lives are stored in computers, which almost anyone can have access to. The feeling is if they don't see it, it isn't there. We remind them of what's there. Some of what's there is good, some is bad."

To make his point, Cruiser asked about an embarrassing and nasty incident last summer involving the reporter and police. Cruiser described it precisely, date and location, indicating he had seen some computer-generated form of the police report. It got the reporter's

Manhattan and called him. We had a brief but cool conversation. As a kid I didn't fit in too much. Spent my elementary years reading, I was into science. In the fifth grade I got into computers. I was a rodent. Those were kids who could do a few rudimentary things with a computer and modem but thought they were God. Now they're called lamers. There's a lot of name-bashing in the computer world."

The beginning of the end of hacking as we know it began in 1986 with the passage of the Computer Fraud and Abuse Act. Some hackers treated it with scorn, others as a challenge. Many saw the legal confusion that would ensue, trying to apply the Constitution to this evanescent form of information and communication. Who prosecutes a computer crime that begins in one state or country and comes to fruition in another? Which legal statutes apply? Who makes legal decisions regarding informational crimes committed through fiber-optic highways of light in the global village? Who will litigate? Who will legislate?

In 1986, the Rocky River police, the FBI and the Secret Service arrested a Rocky River high school student who used his computer to access the office telephone system of several large Cleveland communications companies, charging them thousands of dollars in phone calls. He was made an example through his high-profile arrest, and the news flew through the underground hacker network like greased telepathy. Hours before The Plain Dealer ran the story on Page 1 the next morning, hackers were discussing and passing the news. The litigation had begun.

attention. He asked for some demographic data about Cruiser.

"I grew up in a pretty middle-class-type thing. I live in a middle-class suburb with my parents, I work, commute to college. One of my earliest memories was being 3 years old and playing with the phone. I would keep hitting the hook switch. What I didn't know then was that we had what was called a step line. ... That would change the routing in the central office and they would get on the line and say, 'Can I help you, sir?' and I would laugh and hang up.

"At 10, it occurred to me that it was cool that by using the phone you could talk to anyone in the world who had a phone. I found Isaac Asimov's number in

On November 2, 1988, the computer world received another rude awakening. A graduate student at Cornell University had released the Internet Worm, a program that duplicated itself rapidly, temporarily knocking out more than 155,000 computers and 1,200 separate links that comprise the academic and research network known as Internet. Though Robert T. Morris, the program's designer, intended the worm to be nothing more than a harmless prank, his program went badly awry.

Though no information was lost and no system was damaged, the cost of computer down time was estimated at \$1 million. Morris was the first person convicted of a felony under the Computer Fraud and Abuse Act. He was fined \$10,000 and ordered to complete 400 hours of community service.